

What is claimed is:

1 1. A debug system comprising:
2 a microprocessor operable to store secret program
3 information; and
4 a host computer that is connected to the microprocessor
5 so as to debug the program information in the microprocessor,
6 wherein
7 the microprocessor includes:
8 a nonvolatile memory which (i) has an area for
9 storing key information that is used to securely handle program
10 information and (ii) is writable only once;
11 a writing unit operable to, if no key information
12 is stored in the nonvolatile memory, receive key information
13 from the host computer and write the key information into the
14 nonvolatile memory; and
15 a first transmission unit operable to securely
16 perform transmission of program information with the host
17 computer using the key information that has been written into
18 the nonvolatile memory,
19 the key information that has been written into the
20 nonvolatile memory is not readable outside of the
21 microprocessor, and
22 the host computer includes:
23 a receiving unit operable to receive key
24 information from a user;

25 a sending unit operable to store therein the key
26 information received from the user and send the key information
27 to the microprocessor; and

28 a second transmission unit operable to securely
29 perform transmission of program information with the
30 microprocessor using the key information stored in the sending
31 unit.

1 2. A microprocessor which is operable to store secret
2 program information and is connected to a host computer that
3 is used to debug the program information in the microprocessor,
4 comprising:

5 a program information storing unit operable to store the
6 program information which is one of a program, data and a program
7 and data;

8 an executing unit operable to read the program information
9 to perform an operation corresponding to the read program
10 information;

11 a nonvolatile memory which (a) has an area for storing
12 key information that is used to securely handle program
13 information and (b) is writable only once;

14 a writing unit operable to, if no key information is stored
15 in the nonvolatile memory, receive key information from the host
16 computer and write the received key information into the
17 nonvolatile memory; and

18 a transmission unit operable to securely perform
19 transmission of program information with the host computer using
20 the key information that has been written into the nonvolatile
21 memory, wherein
22 the key information that has been written into the
23 nonvolatile memory is not readable outside of the microprocessor.

1 3. The microprocessor of Claim 2, wherein
2 the nonvolatile memory additionally stores therein flag
3 information that indicates whether key information is stored
4 in the nonvolatile memory,
5 the transmission unit reads the flag information, and
6 if the read flag information indicates that no key
7 information is stored in the nonvolatile memory, the writing
8 unit receives the key information from the host computer, and
9 writes the key information received from the host computer into
10 the nonvolatile memory.

1 4. The microprocessor of Claim 3, wherein
2 the transmission unit includes:
3 an encryption unit operable to encrypt the program
4 information stored in the program information storing unit using
5 the key information that has been stored in the nonvolatile
6 memory; and
7 an output unit operable to output the encrypted program

8 information.

1 5. The microprocessor of Claim 4, wherein
2 the transmission unit further includes
3 an inhibition unit operable to, in response to a request
4 from the host computer, inhibit the output unit from outputting
5 the encrypted program information.

1 6. The microprocessor of Claim 4, wherein
2 the transmission unit further includes:
3 an inhibition condition storing unit storing an inhibition
4 condition that relates to the key information received from the
5 host computer; and
6 an inhibition unit operable to, if the key information
7 received from the host computer satisfies the inhibition
8 condition, inhibit the output unit from outputting the encrypted
9 program information.

1 7. The microprocessor of Claim 3, wherein
2 the program information stored in the program information
3 storing unit is encrypted program information which is one of
4 an encrypted program, encrypted data, and an encrypted program
5 and encrypted data,
6 the executing unit (i) reads the key information that has
7 been stored in the nonvolatile memory, (ii) decrypts the

8 encrypted program information using the read key information
9 so as to generate decrypted program information which is one
10 of a decrypted program, decrypted data, and a decrypted program
11 and decrypted data, and (iii) performs an operation corresponding
12 to the decrypted program information, wherein
13 the transmission performed by the transmission unit is
14 transmission of encrypted program information.

1 8. The microprocessor of Claim 5, wherein
2 the executing unit encrypts a result of the operation using
3 the key information that has been stored in the nonvolatile memory,
4 and writes the encrypted result into the program information
5 storing unit.

1 9. The microprocessor of Claim 5, wherein
2 the program stored in the program information storing unit
3 is an encrypted program, and
4 the program information storing unit has a path to
5 communicate with an external device.

1 10. The microprocessor of Claim 5, wherein
2 the key information that has been written into the
3 nonvolatile memory is constituted by one or more pieces of partial
4 key information,
5 the program stored in the program information storing unit

6 is a plurality of encrypted partial programs each of which
7 corresponds to any of the pieces of partial key information,
8 and
9 the executing unit (a) reads a piece of partial key
10 information from the nonvolatile memory, (b) reads one or more
11 of the encrypted partial programs corresponding to the read piece
12 of partial key information, from the program information storing
13 unit, (c) decrypts the read encrypted partial programs using
14 the read piece of partial key information to generate decrypted
15 partial programs, and (d) performs an operation corresponding
16 to the decrypted partial programs.

1 11. The microprocessor of Claim 3, further including
2 a cache memory, wherein
3 the program information stored in the program information
4 storing unit is encrypted program information which is one of
5 an encrypted program, encrypted data, and an encrypted program
6 and encrypted data,
7 the executing unit (a) reads the key information that has
8 been stored in the nonvolatile memory, (b) decrypts the encrypted
9 program information using the read key information so as to
10 generate decrypted program information which is one of a
11 decrypted program, decrypted data and a decrypted program and
12 decrypted data, (c) writes the decrypted program information
13 into the cache memory, (d) reads the decrypted program

14 information from the cache memory in accordance with a processing
15 speed of the executing unit, and (e) performs an operation
16 corresponding to the decrypted program information, and
17 the transmission performed by the transmission unit is
18 transmission of encrypted program information.

1 12. The microprocessor of Claim 2, wherein
2 the nonvolatile memory additionally stores flag
3 information indicating whether the key information is stored
4 in the nonvolatile memory,
5 the transmission unit reads the flag information,
6 if the read flag information indicates that no key
7 information is stored in the nonvolatile memory, the transmission
8 unit reads the program information from the program information
9 storing unit and outputs the read program information to the
10 host computer, and
11 if the read flag information indicates that the key
12 information has been stored the nonvolatile memory, the
13 transmission unit reads the program information from the program
14 information storing unit, encrypts the read program information
15 using the key information that has been stored in the nonvolatile
16 memory, and outputs the encrypted program information to the
17 host computer.

1 13. A host computer which (i) is connected to a

2 microprocessor operable to store secret program information and
3 (ii) debugs the program information in the microprocessor,
4 comprising:
5 a receiving unit operable to receive key information from
6 a user;
7 a sending unit operable to store the received key
8 information therein and send the received key information to
9 the microprocessor; and
10 a transmission unit operable to securely perform
11 transmission of program information with the microprocessor
12 using the key information stored in the sending unit.

1 14. The host computer of Claim 13, wherein
2 the transmission unit includes:
3 a program information receiving unit operable to receive,
4 from the microprocessor, encrypted program information which
5 has been generated by encrypting the program information;
6 a decrypting unit operable to decrypt the encrypted program
7 information using the key information stored in the sending unit
8 so as to generate decrypted program information; and
9 a display unit operable to display the decrypted program
10 information generated by the decrypting unit.

1 15. The host computer of Claim 14, wherein
2 the transmission unit further includes:

3 a program information input unit operable to receive, from
4 the user, program information which is one of a program, data
5 and a program and data;

6 an encrypting unit operable to encrypt the program
7 information received from the user, using the key information
8 stored in the sending unit so as to generate encrypted program
9 information; and

10 an output unit operable to output the encrypted program
11 information generated by the encrypting unit to the
12 microprocessor.

1 16. The host computer of Claim 14, further comprising:

2 a storage unit storing a source program;

3 a conversion unit operable to convert the source program
4 into an object program; and

5 an encrypting unit operable to encrypt the object program
6 using the key information stored in the sending unit so as to
7 generate an encrypted program, wherein

8 the transmission unit transmits the encrypted program
9 generated by the encrypting unit to the microprocessor.

1 17. The host computer of Claim 14, wherein

2 the transmission unit further includes:

3 an inhibition condition storing unit storing an inhibition
4 condition that relates to the key information; and

5 an inhibition request output unit operable to, if the key
6 information satisfies the inhibition condition, output a request,
7 to the microprocessor, to inhibit the transmission of the
8 encrypted program information.

1 18. A read/write device that is connected to a
2 microprocessor operable to store secret program information,
3 comprising:
4 a receiving unit operable to receive key information from
5 a user;
6 a sending unit operable to store the received key
7 information therein and send the received key information to
8 the microprocessor; and
9 a transmission unit operable to securely perform
10 transmission of program information with the microprocessor
11 using the key information.